Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2010 Proceedings

Americas Conference on Information Systems (AMCIS)

8-2010

Good Practice Guide for Managing IT Risk in Colombian Banking: Specification by Disciplines

Camilo Méndez Ayerbe
Universidad de los Andes, camilo.mendez.ayerbe@gmail.com

Gustavo Camargo Avendaño
Universidad de los Andes, gu-camar@uniandes.edu.co

Andrea Herrera
University of Auckland, anhesue@gmail.com

Good Practice Guide for Managing IT Risk in Colombian Banking: Specification by Disciplines

Camilo Méndez Ayerbe
Universidad de los Andes
c-mende1@uniandes.edu.co

Gustavo Camargo Avendaño
Universidad de los Andes
gu-camar@uniandes.edu.co

Andrea Herrera Suescún
Universidad de los Andes
a-herrer@uniandes.edu.co

ABSTRACT

In this paper, we describe the work, findings, study case and contributions made in the development of the specification of the "Guía de buenas prácticas de gestión de riesgo de TI en el sector bancario colombiano"[1]. We present how doing the specification of the most important step of the guide, makes it a strong tool for managing IT risk in the Colombian banking sector. This was achieved by reviewing some of the most relevant theories in IT risk management, developing new models that exploit their best attributes, and presenting them from a business point of view. Finally, we present the results obtained from validating the new constructed models in our study case: the cheque clearing process of "Banco de la República"[2]; a core service in the organization that depends ninety percent on IT.

Keywords

IT Risk Management, Models, Disciplines, Foundation, Governance, Culture, 4-A, Study case, Bank, Service.

INTRODUCTION

Any enterprise has to develop its business core as its prime objective, and they model it through processes and services. IT has increasingly been incorporated as part of the processes and services. While these tendencies started to grow, they became more complex and the probability of having problems increased; this is a risk. Managing risk and being prepared is a relative new concept. The financial sector was the first to start talking about it and managing it (12).

An appropriate IT risk management will allow an adequate use of IT resources and a convenient information management; the potential opportunities of doing so will benefit the processes and services in the business. Attacking this issue has been done by some universities and bodies[3]; they have developed tools to manage the IT risk from different points of view, but there is still some work to be done. Having this in mind, we took the guide (4), which was constructed with some of these theories, and we specified and reinforced it with models developed specifically for it, making it a better tool.

In order to validate the new models we developed a study case. We worked with the central bank called "Banco de la República (BR)", which trends on subjects such as continuity and risk management. The Bank has been a pioneer on the implementation of new initiatives, using IT in their services and processes.

To show the way this work was done, we will start by introducing the existing frameworks; then we will explain how these frameworks are used to develop the new models. Finally, we will illustrate the models and how they became part of the studies developed at University of Los Andes and their validation at BR. Let's start reviewing the models.

---

[1] Good practices guide for managing IT risk in Colombian banking

[2] The central bank of Colombia

[3] Like MIT, ISACA and more.

STATE OF ART AND MODELS DEVELOPED

The idea of managing risk from a business point of view comes from a number of frameworks developed by universities and corporations in search of making IT problems and solutions a business concern[4]. An initiative on this regard is the Good Practices Guide for IT Risk Management in Colombian Banking (4). This was developed from a theoretical model which integrates three frameworks taking advantage of their main strengths, and the existing regulations for banking in Colombia (15), which respond to a parent subsidiary model. However, this guide does not have enough tools that support the definition of specific actions to meet the needs of an organization; for this reason, we specified this guide with new models. We built the models according to the 4-A framework (17), complemented for the Risk IT (9) framework created by the ITGI[5], and some other authors and documents related to the IT risk topic, making them a strong base for the guide specification.

The guide (Image 1) contains six steps (4): build the ideal profile of IT risk, define the actual IT risk profile, prioritize of discipline, detail and plan the development of the discipline, grade implemented actions, and feedback. In this paper, we will show the construction, specification and validation of the fourth step, "Planeación detallada de desarrollo de cada disciplina"[6], because it is the step necessary to define the actions roadmap to mature risk management.

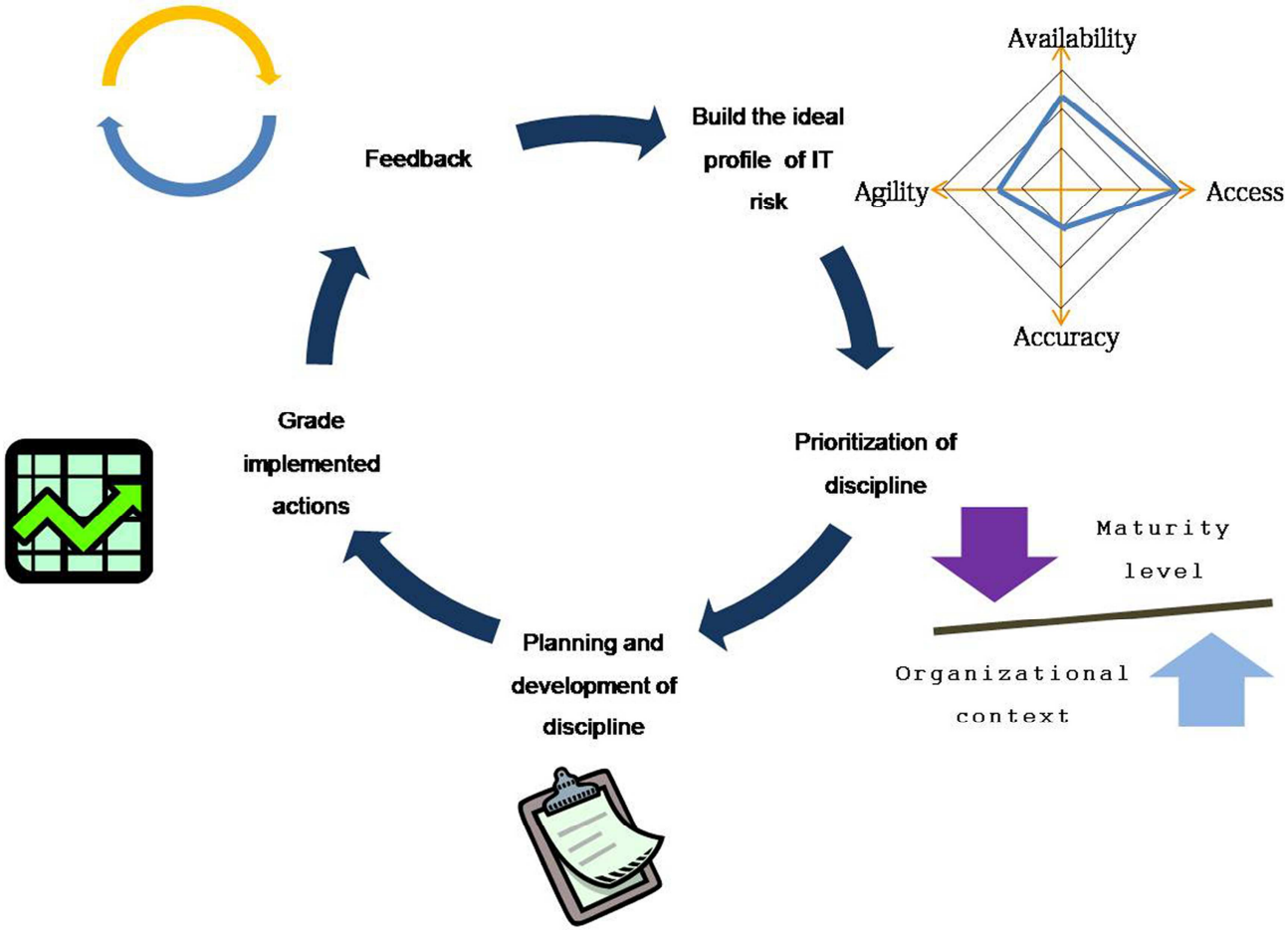

Image 1. Guide for managing IT risk in Colombian banking. (4)

[4] IT risk (17), Risk IT (9), among others.

[5] IT Governance Institute

[6] Detail planning and development of each discipline

In order to build the detailed planning and development of each discipline step, we have to briefly present the main framework for this study, the 4-A. This has in its core four business objectives: Availability, Accuracy, Access and Agility; and three disciplines: Foundation, Governance and Culture (17), all having the same importance and relevance but some with more theory developed than others. With this base framework we started to build cohesive individual models using other frameworks and theories to complement each of the disciplines in the 4-A framework. Here is a brief explanation of the enhanced models that we have built.

Foundations

First of all, it is necessary to define what "the foundation" is; according to Westerman and Hunter, it is "the collection of IT assets, procedures, and people that support and enable business processes and decision making. A weak foundation is the perfect state for materialization of any kind of risk, especially IT risks. Inconsistent software updates and a complex interdependency between components allow systems to fail constantly, make it hard to recover it and even worse, impossible to change" (17). Secondly, a mature foundation is statistically the most important element to reduce risks and improve the IT performance.

Given the fact that IT is transversal to the organization, it is possible to say that its problems are also important; in addition, IT is responsible for the interactions between business units, and among the business with the world. For this reason, it becomes pertinent to identify future problems in order to create methods and measures to avoid those system's failures (17).

Some of the benefits that are possible to develop through an adequate IT risk management guided by a foundation-driven approach, are (17):

- Immediately finding and fixing holes in the foundation corrects immediate weaknesses, providing time to make other longer-term improvements.
- Simplification is the most cost-effective risk management approach over the long term because it pays off in cost reduction as well as in risk reduction.
- Simplification reduces IT risks[7] and makes the other two disciplines easier to master.

According to the framework, a solid IT foundation that has a low risk impact and a low probability of occurrence can be developed following three fundamental steps, all of them visibly related to its strengthening. Those steps are (17):

1. Address availability risk by managing business continuity to ensure that the organization can recover and run again quickly if a major incident occurs.
2. Identify and plug holes in the foundation, using IT audit and the knowledge of the IT team as a guide, to address availability and assess risks.
3. Implement basic IT controls and industry best practices to monitor the status of the base and prevent future holes in the foundation.

Each one of these steps was strengthened with the model developed by the incorporation of deeper theories, as follows:

1. The continuity component was extended by introducing the industry best practices for BCM[8] Program, set of guidelines developed by the BCI[9] (1). We used it because according to specialized and prestigious institutes like the BSI[10]: this standard is one of the most well known and applied guidelines, being used by more than 4,500 members worldwide in more than 85 countries. (2).

   This first step seeks the creation of a high level of awareness about the importance of IT through the organizational internalization of its value, allowing the development of action plans in case of an eventuality that disrupts the normal realization of processes within the organization. The BCM Program guide chosen was the one that better matched the

[7] Related with core four business objectives

[8] Business Continuity Management

[9] Business Continuity Institute

[10] British Standard Institute

theory exposed by the framework 4-A, given that the 4-A proposes three simple steps to build those continuity plans (Image 2).

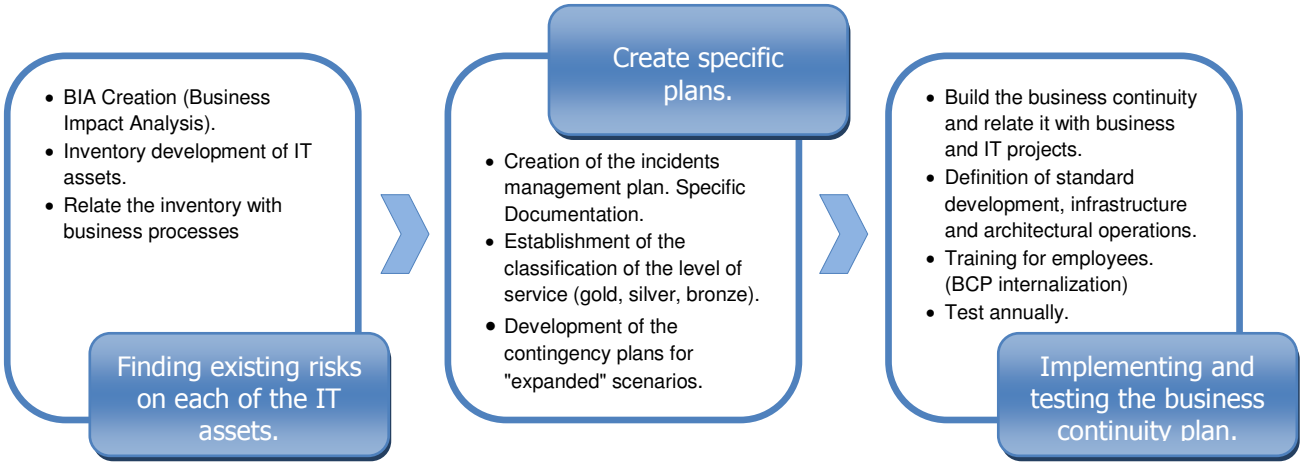

Image 2. Key Steps BCP

2. The finding and fixing infrastructure failures element was built combining elements from the first and the third components.

   In general, when something from IT fails, whether by human actions or IT breakdowns, without endangering the business continuity, it is considered as a minor error or failure. Those "ordinary problems" become part of the employee's tasks, making them invisible to the risk and continuity management, and the big danger is the sum of those minor errors resulting in enormous problems.

   First of all, it is necessary to identify the failures and the scenarios of risks, by analyzing the historical data and looking at the plans of continuity existing within the organization. Once those are identified, an audit of all the processes involved must be carried out.

   To do this as the framework recommends, and in order to improve the theory, the model adds elements from the guidelines of BCM Program (1) that are strongly related to finding holes in the infrastructure, and elements from ITIL[11] (10) that are focused on changing and managing the infrastructure, (Image 3). ITIL was chosen because is one of the three major IT Governance frameworks worldwide together with COBIT [12] (7).

Image 3. Foundation's controls

[11] IT Infrastructure Library

[12] Control Objectives for Information and Related Technologies

3. The IT management component was specified by integrating ITIL (10) and the governance framework COBIT (7) to the framework 4-A to provide a powerful IT governance and control (8), (9).

   Currently there are a great number of standards for IT management and governance, some of them more popular than others. The main reason to use them, even though those controls should be designed and built within the company, is the need to base them on the industry´s standards in order to avoid the generation of new problems. Furthermore, using standards means that the knowledge of experts on a specific subject has been incorporated to the company. Therefore, the third step was decided to be specified and improved by introducing and adding industry ITIL and COBIT standards to the framework. This incorporation allows managing the third component with a more detailed approach.

After doing the research, introducing and integrating all those theories and guidelines in the main model, it can be seen the entire discipline of foundation as a fortified set of steps and practices that will allow, improving the infrastructure management and consequently the IT risk management, (Image 4).

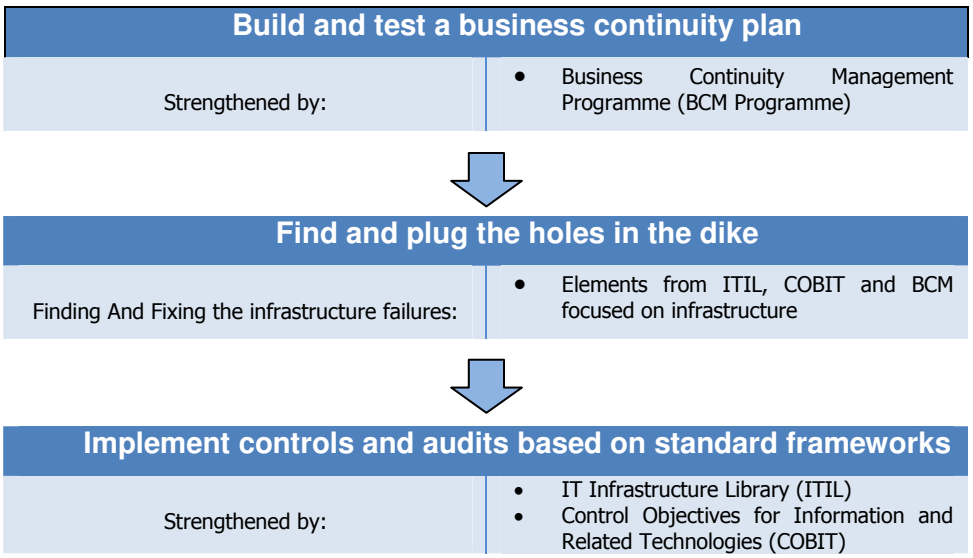

Image 4. Foundation model (11)

This covers the basic information about the new foundation model (11). Next, the risk governance discipline.

Risk Governance

The model for IT risk governance discipline was built from two frameworks, starting from the comparative analysis that allowed selecting the framework 4-A as the main one and the "Risk IT" framework (9), which is fully integrated with COBIT and is a good complement for operative matters.

The 4-A IT risk governance discipline is composed by three main elements: a cyclic process, which identifies IT risk and monitors the way those risks evolve, and develops standards and policies to manage them; a structure of roles and responsibilities; and defined best practices.

Then, this discipline defines which of the risks are within the organization; it monitors them, prioritizes them, and develops politics and methods to manage them through different roles and practices of process improvement as represented in image 5.

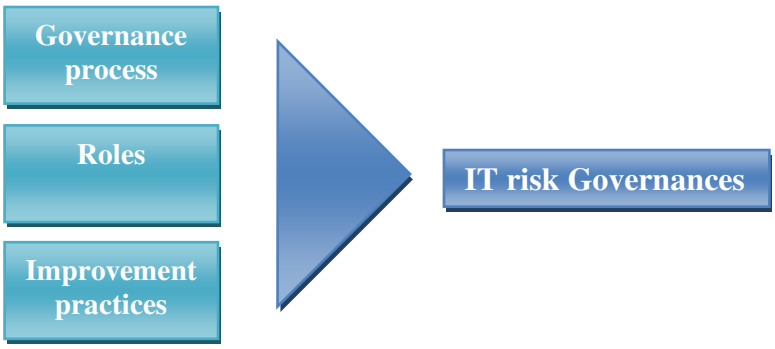

Image 5. Government IT Risk Management[13]

The 4-A framework gives us the information on how to start a development of the governance discipline, but to make our model better, we use the three domains that come from the Risk IT framework. We try to take advantage of operative point of view that present Risk IT merging it with the three elements of 4-A. This way we have both, the strategic and operative vision that gives us a better and wider tool to use. And by doing so, we obtain the governance model (Image 6).

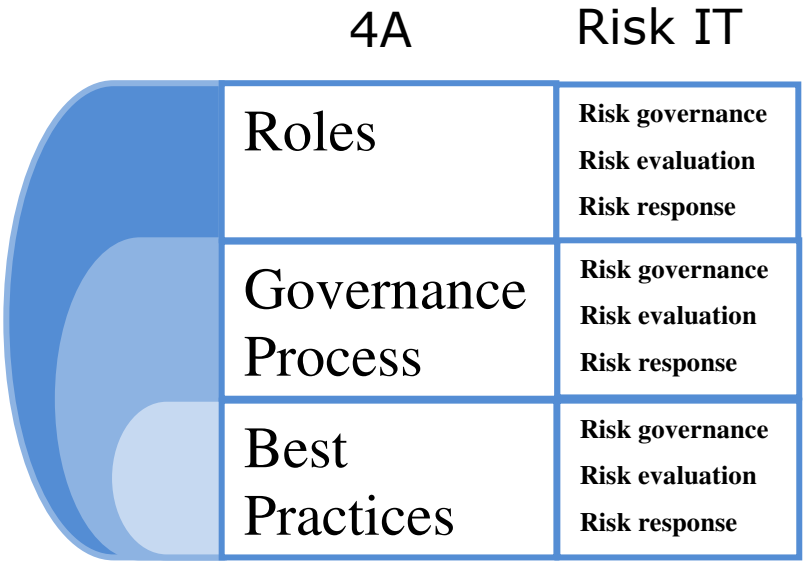

Image 6. Governance model (11)

This figure shows how the domains of Risk IT Framework, which has an operational standpoint, complement and support the business point of view proposed by the framework 4-A. Each of the proposed activities in the domains of Risk IT framework fits into any of the components of the framework governing discipline, 4-A, and facilitates the planning and developing actions that will improve the processes.

Culture

The original 4-A framework that we took as basis, has an approach to the discipline of culture that is not specific in terms of evaluation and development but it establishes an ideal state of what it is desired for a risk culture. Some of the desired behaviors are (17):

It is ok to talk about risk.

---

13 Transformed from "Especificación por Disciplinas de la Guía de buenas prácticas en gestión de riesgos de TI en el sector bancario colombiano."(4) Page 55, figure 18.

-
- It is ok to take risks.
- Success and failures are tracked and analyzed.
- There is continuous learning an improvement of key processes.
- Realistic budgets and timelines that are continuously monitored.
- The enterprise is able to take on bigger risks.

We identified some guidelines and behaviors but not a way to measure it, but we needed to grow risk culture into something measurable and evaluable. Therefore, we searched in other fields with experience analyzing and studying culture like marketing and anthropology, to find guidelines to create our model. We used some of the renowned authors and theories in these academic disciplines regarding culture and selected the ones that helped us grow the guidelines.

Achieving these behaviors is how any enterprise will obtain its culture risk awareness. The difficulty lies on how to get there. First, it is necessary to understand that culture is something that exists in every human being; it is transferred from the society to the person since birth and can be very different from one person to other (13). Knowing this makes the understanding of the way an organization culture behaves independent of the rules it has defined and it can differ from its hierarchic structure. In this social hierarchy there are leaders and followers, and that may differ from one organization to another. The question then is, how to make the culture of an organization be aligned with its organizational rules and ideas?

To do this it is necessary to create effective communication channels, for broadcasting the way the organization wants its people to behave. Using a simple communication model, the behavior can be broadcasted (3). The next step is defining how and what the organization wants to communicate.

The "how" could be define by three practices that develop risk culture awareness. 1. The first approach emphasizes the importance of instilling security behavior into daily work practices; 2. The second suggests education and training processes to internalize security aspects and shape behavior; 3. And the last focuses on social participation and motivation as means of achieving compliance with formal mechanisms (5).

The "what" in culture is defined by what information is public and what is private, what is spoken and what is not, and what is explicit or what is implicit (6). Defining information in these terms allows the mapping of the way the culture in the organization behaves. Also, with cross referencing between the practices presented earlier, we can value the acceptance of a risk element, (table 1).

Cultural Analysis									
Element to evaluate	Practice	Private				Public			
		Not speak		Speak		Not speak		Speak	
		implicit	explicit	implicit	Explicit	implicit	explicit	implicit	explicit
Element 1	1								
	2								
	3								

Table 1. Cultural model (11)

This new model gives a solid base to develop risk culture awareness in an organization (11).

The three models were verified through the creation of a check list, needed to complete the fourth step of the guide (4). We present the models' validation in the next segment.

STUDY CASE

The validation of the models was done studying and analyzing a single process. This was made in BR with the cheque clearing process.

Bank and process description

Banco de la República

The Bank was created in 1923 to be the Central Bank of Colombia. This institution has the responsibility of acting as State Bank; of controlling the issue of legal tender; of receiving allocations of credit and providing loans to commercial banks and the Government; and of managing and directing the country's monetary (inflation controls) and financial policy; amongst other functions (14).
In the Bank, the "Unidad de Riesgo Operativo y Continuidad" [14] (UROC) and the "Subgerencia Informática" (IT VP) are responsible for managing IT risk. The UROC is responsible for all the operative risks in the Bank, and the IT VP is responsible for all the IT of the Bank. The other unit that was involved in this study was the business area named "Subgerencia de operación bancaria"[15] (BO VP), this unit is the owner of the business process studied.

Cheque clearing process

It is the process in which all banks in the nation cross the checks that arrive to them from other banks and change their accounts state. The process depends on a system called "Compensación Electrónica de Cheques"[16] (CEDEC). Other systems that are involved in the process are: "Sistemas Electrónicos del Banco de la República"[17] (SEBRA), "Cuentas de Depósito"[18] (CUD), and "Transmisión de Archivos Segura"[19] (HTRANS) (11).

The specification by disciplines

In the guide before the forth step, it is necessary to identify which discipline has priority to develop. The guide provides a tool to do so (4). As a result, that discipline is detailed. In this study case, the discipline with highest priority was governance, but each discipline was developed to apply the models built. The detail and plan of the discipline step has two sections. The first part is the application of a checklist, based on the models, to the units involved. After evaluating each checklist we take the results and develop an action plan that creates a roadmap to mature each discipline.

Findings and proposals

Here there is a brief explanation of the results obtained in the validation of each discipline and a description of the respective action plan.

Foundation

The largest part of this validation was carried out with the IT VP by using the instrument created, more precisely with the informatics continuity and support unit. However, the validation itself and this instrument were firstly adjusted with the UROC. The results shown by the posterior analysis of the checklist were as follows:

Build and test a business continuity plan: The continuity unit of the Bank has been working on it during several years; it can be seen on the continuity plan that is already implemented. Even though not all the activities proposed by the checklist-model are been carried out, the majority of them are already been done. In fact, just two activities are in process of elaboration and those are the interdependencies between activities identification, and the identified threats prioritization. This is because the initiative for unifying the IT risk management at the Bank started short time ago; it is still a newborn process. Now, it is

[14] Operative Risk and Continuity Unit

[15] Banking operation VP

[16] electronic cheque clearing

[17] Republic Bank electronic systems

[18] Deposit accounts system

[19] Secure file transmission

important to say that even though there were business units already doing risk management, it was not done according to an organizational standard, so it is the reason why these two activities that involve more than one unit are still being developed.

Finding and repairing IT failures: The complete set of activities planned on the checklist has been developed in the Bank during several years. The reason is that a large proportion of those activities are related to operative tasks. For example, identifying infrastructure failures is already part of the duties of operative units. According to the analysis carried out by validating the checklist, this step is highly performed in the Bank (as much in operative levels as executive levels), moreover the Bank has an extensive experience at finding and repairing IT failures due to its multiple initiatives on embracing periodically cutting edge technologies and maintaining the mature ones.

Implementing controls and audits based on standard models: This last step of strengthening the foundation is the one that has been less developed; a considerable amount of activities are still in process of implementation because the IT risk management is somehow a new model of IT administration for the Bank. It is reasonable to point out that all of the activities are already developed or are in a developing stage in the Bank. This part of fixing the foundation is more associated with executive process whereas the continuity part is more connected to operative process, for this reason, one is more developed than the other at the moment. Looking at this step in detail:

- The service transition is the stage of IT management that has more activities in process; this is because the infrastructure involved in the cheque clearing process does not change frequently.
- The cheque clearing process is a static process that does not require constant technology innovation because of that efforts are focused on ensuring the infrastructure availability.

To sum up, the business continuity management and the finding and fixing infrastructure failures are the most developed steps in fixing the foundation at the moment. The continuity plan of the bank is built by a set of best practices created by the DRII[20]. This part of the guide is based on good practices published by the BCI even though these are very similar and easy to compare.

Also the IT VP of the bank is driven by two sets of best practices called ITIL and COBIT, exactly the same sets of best practices chosen to specify this guide and complement the theory given by the framework 4-A.

Governance Process Discipline

The validation of this discipline covers not only the cheque clearing process but the entire sets of process that involves IT within the organization. This is the reason why its components have a corporate reach.

The results were obtained through direct interviews to employees linked to the cheque clearing process. The interviewees were two senior engineers from the quality area and an expert engineer from the UROC. The data obtained was analyzed with the instrument built in the specification of the guide and gave us the following results.

The roles are well structured within the entire organization. Although the roles names defined within the Bank not always match with those proposed, its functions and responsibilities are very similar and sometimes equal.

Reviewing the governance component, we found that as a new unit, the UROC has been defining processes but not all of them have established clear metrics and monitoring. Once the IT risks are clearly identified, the IT VP defines its own processes to handle them. However, these processes are being revised in order to unify them with the model built by the UROC. At the moment the IT VP is focused in security, availability and projects risks.

Once the third component was validated, it was found that the Bank uses the best practices of the banking sector as Basel, as well as IT management best practices such as COBIT, ITIL and project management. It is important to evaluate the level of customization of each model.

In conclusion, it can be seen that in the BR the risk management in general has been implemented over several years and moreover, the IT risks management has become an important issue; making important to mature this discipline inside the Bank.

[20] Disaster Recovery International Institute

Culture

From the culture model, we have designed five components that evaluate the most important behaviors in risk culture. These components are:

- Organizational culture.
- Social culture.
- Politics and rules.
- Training and awareness campaigns.
- Cultural acceptance.

Each component contains a number of questions that allowed us to validate it and identify the aspects in which the Bank needs to work. The evaluation was done in all the units that have a relation with the process. The two components that got the lower score were: the politics and rules and, training and awareness campaigns. In each component a number of actions were proposed to the Bank for implementation that will mature them.

Politics and rules: as the unit responsible for managing risk, the UROC has developed a set of norms that are known through all the process, but specially the rules are too general and the process has different types of people involved. Also the jobs descriptions do not have specific information to generate risk awareness and notify what part of the information is public or private.

Training and awareness campaigns: The UROC and the IT VP have developed training programs and campaigns that take care of generating risk awareness, but as the previous component they are too general.

These plans have been presented to the Bank with more extensive description of the actions to develop. (11)

Because this study is the development of the detail planning and development of each discipline, after each of the disciplines were validated, we developed a cross reference for the study case showing how working in an specific action in the governance plan can take effect in foundation or in culture (11) making this the final development of the study.

CONCLUSIONS

This study has two big components: the construction of the models that support and detail the "planning and development of each discipline step" for the guide, and the validation of this step in the Bank's process. Through the first part, we contributed to one of today's engineering challenges in the field of security (16), and with the study case we started the validation of our scientific approach.

In BR, we found that being the Central Bank of Colombia, they are aware of the necessity and value that IT can bring to their processes and that an effective risk management can bring them a better return from their IT investment. This is due to their work in obtaining a mature state in IT risk management. Through this maturity they obtain a better efficiency from their processes and overall the banking business´. Furthermore, due to the importance and relevance that BR has as a national institution, they must make their continuity plans strong and well built. This is the goal that BR wanted to accomplish by giving us access to its process.

With the specification of the guide adding high standards and theories developed by world class institutions and organizations, we hope it will be a useful tool for the organizations in the business, in the near future, by making this specification a valuable way to analyze, rate and manage the risk that comes from IT. Thus, the business will gain more value from IT processes.

The development of the models was a journey that was possible due to the recollection of information and the search for theories that enhance and extend the existing frameworks. We developed these models not by thinking of what has been done and said in IT risk management, but by trying to find was is not been said and done in this field. We used the existing materials, theories, and frameworks from other fields, even some not related with IT to make something better. This gives us a result that, viewing the problem from diverse angles, can bring a better solution.

The specification has been proved in a study case. Therefore, it could be extended to other types of banks and other kinds of companies in the financial sector in order to have more solid evidence of its validity.

The idea of applying IT risk management in IT process or IT depending processes will make a business gain better value of their IT. Using the models developed in this project will help to identify and plan the step toward getting a managed risk environment and give a point of balance in a world were chaos and uncertainty are not uncommon. Hence, being prepared may make the difference.

REFERENCES

1. Business Continuity Institute. (2008) *Good Practices Guidelines*. United Kingdom: Business Continuity Institute. http://www.thebci.org/gpg.htm
2. British Standards Institute. (2010) *About Business Continuity Institute (BCI),* http://www.bsigroup.com/en/About-BSI/News-Room/BSI-News-Content/Disciplines/Business-Continuity/BSI-supports-BCI-conference/
3. Corella, M. A., & Reséndiz, C. R. (2008) *El poder de la comunicación en las organizaciones.* Plaza y Valdes.
4. Figueroa, L. C. (2010) *Guía de buenas prácticas de gestión de riesgo de TI en el sector bancario Colombiano.* Bogotá: Universidad de los Andes.
5. Garzon, A. (2007) *Information security culture: the effect of institutional factors and the mediating role of business continuity practices.* London.
6. Hall, E. T. (1976) *Más allá de la cultura.* Barcelona: Editorial Gustavo Gili, SA.
7. ISACA. (2009) *COBIT 4.1* http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/CobiT4.1_Brochure.pdf
8. ISACA. (2005) *Cobit como estandar de seguridad* http://www.itgi.org/Template.cfm?Section=Home&CONTENTID=24700&TEMPLATE=/ContentManagement/ContentDisplay.*cfm*
9. IT Governance Institute. (2009) *Enterprise Risk: Identify, Govern and Manage IT Risk.* s.l. : http://www.isaca.org/Template.cfm?Section=Risk_IT7&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=79&ContentID=48749
10. IT-processmaps. (2009) *ITIL Process Maps*. Recuperado el 28 de 10 de 2009, de http://en.it-processmaps.com/products/itil-process-map.html
11. Méndez, C., & Camargo, G. (2009) *Especificación por Disciplinas de la Guía de mejores prácticas en gestión de riesgos de TI en el sector bancario colombiano.* Bogotá: Universidad de los Andes.
12. Pérez, I. (2009) Riesgo Operativo. *Semana del ROC (riego operativo y continuidad).* Bogota: Banco de la republica.
13. Rapaille, C. (2007) *El Código Cultural.* Editorial Norma.
14. República, B. d. (2009) *History*. www.banrep.gov.co.
15. Supernintendencia Financiera de Colombia. (2007) "*Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios"* http://www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ce052_07.rtf
16. University of Southen California. (2010) *Viterbi Research on the NAE Grand Challenges*, http://viterbi.usc.edu/research/grand-challenges/
17. Westerman, G., & Hunter, R. (2007) *IT Risk: Turning business threats into competitive advantage.* Boston, Massachusetts: Harvard Business School Press.